(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－89669
（P2000－89669A）
(43)公開日　平成12年３月31日(2000.3.31)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ｚ	

審査請求　未請求　請求項の数10　ＯＬ　（全８頁）

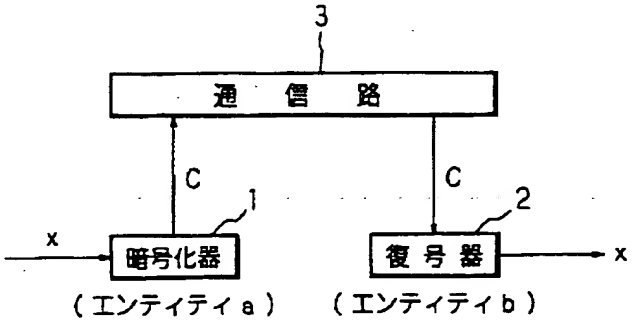
(21)出願番号　特願平10－262037

(22)出願日　平成10年９月16日(1998.9.16)

(71)出願人　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地
(71)出願人　597008636
笠原　正雄
大阪府箕面市粟生外院４丁目15番３号
(72)発明者　笠原　正雄
大阪府箕面市粟生外院４丁目15番３号
(72)発明者　村上　恭通
京都府京都市伏見区竹田向代町136番地
村田機械株式会社本社工場内
(74)代理人　100078868
弁理士　河野　登夫

(54)【発明の名称】　暗号化方法，復号方法，暗号化・復号方法及び暗号通信システム

(57)【要約】
【課題】　高速の復号が可能な積和型暗号の暗号化・復号方法を提供する。
【解決手段】　平文ベクトルm＝（m_0，m_1，…，m_{K-1}）と基数ベクトルD＝（D_0，D_1，…，D_{K-1}）とを用いた内積により暗号文$C=m_0 D_0+m_1 D_1+\cdots+m_{K-1} D_{K-1}$を得る積和型の暗号方式であって、$D_i$（$0 \leqq i \leqq K-1$）を$D_i=d/d_i$（但し、$d=d_0 d_1 \cdots d_{K-1}$（任意の２つの数$d_i$，$d_j$は互いに素））に設定する。



1

【特許請求の範囲】

【請求項１】　平文をＫ分割した平文ベクトルｍ＝（ｍ$_0$，ｍ$_1$，…，ｍ$_{K-1}$）と基数ベクトルＤ＝（Ｄ$_0$，Ｄ$_1$，…，Ｄ$_{K-1}$）とを用いて暗号文Ｃ＝ｍ$_0$Ｄ$_0$＋ｍ$_1$Ｄ$_1$＋・・・＋ｍ$_{K-1}$Ｄ$_{K-1}$を得る暗号化方法において、前記Ｄ$_i$（０≦ｉ≦Ｋ－１）をＤ$_i$＝ｄ／ｄ$_i$（但し、ｄ＝ｄ$_0$ｄ$_1$…ｄ$_{K-1}$（任意の２つの数ｄ$_i$，ｄ$_j$は互いに素））に設定することを特徴とする暗号化方法。

【請求項２】　平文をＫ分割した平文ベクトルｍ＝（ｍ$_0$，ｍ$_1$，…，ｍ$_{K-1}$）と基数ベクトルＤ＝（Ｄ$_0$，Ｄ$_1$，…，Ｄ$_{K-1}$）とを用いて暗号文Ｃ＝ｍ$_0$Ｄ$_0$＋ｍ$_1$Ｄ$_1$＋・・・＋ｍ$_{K-1}$Ｄ$_{K-1}$を得る暗号化方法において、前記Ｄ$_i$（０≦ｉ≦Ｋ－１）をＤ$_i$＝（ｄ／ｄ$_i$）・ｖ$_i$（但し、ｄ＝ｄ$_0$ｄ$_1$…ｄ$_{K-1}$（任意の２つの数ｄ$_i$，ｄ$_j$は互いに素），ｖ$_i$：乱数）に設定することを特徴とする暗号化方法。

【請求項３】　乱数ベクトルｖ＝（ｖ$_0$，ｖ$_1$，…，ｖ$_{K-1}$）を用いて暗号文Ｃ＝ｍ$_0$ｖ$_0$Ｄ$_0$＋ｍ$_1$ｖ$_1$Ｄ$_1$＋・・・＋ｍ$_{K-1}$ｖ$_{K-1}$Ｄ$_{K-1}$を得る請求項１記載の暗号化方法。

【請求項４】　請求項１，２または３によって暗号化された暗号文Ｃに対して、中間復号文Ｍを式（ｄ）のようにして求めるステップと、

Ｍ≡ｗ$^{-1}$Ｃ　(mod Ｐ)　…（ｄ）

この中間復号文Ｍを以下の式（ｅ）により復号して平文ベクトルｍ＝（ｍ$_0$，ｍ$_1$，…，ｍ$_{K-1}$）を求めるステップと

ｍ$_i$≡ＭＤ$_i$$^{-1}$　(mod ｄ$_i$)　…（ｅ）

を有することを特徴とする暗号化・復号方法。

【請求項７】　平文をＫ分割した平文ベクトルｍ＝（ｍ$_0$，ｍ$_1$，…，ｍ$_{K-1}$）と基数ベクトルＤ＝（Ｄ$_0$，Ｄ$_1$，…，Ｄ$_{K-1}$）とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、

Ｃ＝ｍ$_0$ｃ$_0$＋ｍ$_1$ｃ$_1$＋・・・＋ｍ$_{K-1}$ｃ$_{K-1}$　…（ｈ）

暗号文Ｃに対して、中間復号文Ｍを式（ｉ）のようにして求めるステップと、

Ｍ≡ｗ$^{-1}$Ｃ　(mod Ｐ)　…（ｉ）

この中間復号文Ｍを以下の式（ｊ）により復号して平文ベクトルｍ＝（ｍ$_0$，ｍ$_1$，…，ｍ$_{K-1}$）を求めるステップと

ｍ$_i$≡ＭＤ$_i$$^{-1}$　(mod ｄ$_i$)　…（ｊ）

を有することを特徴とする暗号化・復号方法。

【請求項８】　平文をＫ分割した平文ベクトルｍ＝（ｍ$_0$，ｍ$_1$，…，ｍ$_{K-1}$）と基数ベクトルＤ＝（Ｄ$_0$，Ｄ$_1$，…，Ｄ$_{K-1}$）とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、

2

＊れた暗号文Ｃを復号する復号方法であって、以下の式（ａ）により平文ベクトルｍ＝（ｍ$_0$，ｍ$_1$，…，ｍ$_{K-1}$）を求めることを特徴とする復号方法。

ｍ$_i$≡ＣＤ$_i$$^{-1}$　(mod ｄ$_i$)　…（ａ）

【請求項５】　前記Ｋ個のｄ$_i$の集合を複数組準備し、それぞれの集合毎に暗号文を得るようにした請求項１または２記載の暗号化方法。

【請求項６】　平文をＫ分割した平文ベクトルｍ＝（ｍ$_0$，ｍ$_1$，…，ｍ$_{K-1}$）と基数ベクトルＤ＝（Ｄ$_0$，Ｄ$_1$，…，Ｄ$_{K-1}$）とを用いて前記平文を暗号文に変換し、その暗号文を元の平文に変換する暗号化・復号方法において、

前記Ｄ$_i$（０≦ｉ≦Ｋ－１）を整数ｄ$_i$を用いてｄ／ｄ$_i$（但し、ｄ＝ｄ$_0$ｄ$_1$…ｄ$_{K-1}$（任意の２つの数ｄ$_i$，ｄ$_j$は互いに素））に設定するステップと、

ｗ＜Ｐ（Ｐ：素数）を満たすｗを選択し、式（ｂ）により公開鍵ベクトルｃ＝（ｃ$_0$，ｃ$_1$，…，ｃ$_{K-1}$）を求めるステップと、

ｃ$_i$≡ｗＤ$_i$　(mod Ｐ)　…（ｂ）

平文ベクトルｍと公開鍵ベクトルｃとの内積により、式（ｃ）に示す暗号文Ｃを作成するステップと、

＊

Ｃ＝ｍ$_0$ｃ$_0$＋ｍ$_1$ｃ$_1$＋・・・＋ｍ$_{K-1}$ｃ$_{K-1}$　…（ｃ）

※前記Ｄ$_i$（０≦ｉ≦Ｋ－１）を式（ｆ）にて設定するステップと、

Ｄ$_i$＝（ｄ／ｄ$_i$）・ｖ$_i$　…（ｆ）

但し、ｖ$_i$：乱数

ｄ$_i$：整数

ｄ＝ｄ$_0$ｄ$_1$…ｄ$_{K-1}$

（任意の２つの整数ｄ$_i$，ｄ$_j$は互いに素）

ｗ＜Ｐ（Ｐ：素数）を満たすｗを選択し、式（ｇ）により公開鍵ベクトルｃ＝（ｃ$_0$，ｃ$_1$，…，ｃ$_{K-1}$）を求めるステップと、

ｃ$_i$≡ｗＤ$_i$　(mod Ｐ)　…（ｇ）

平文ベクトルｍと公開鍵ベクトルｃとの内積により、式（ｈ）に示す暗号文Ｃを作成するステップと、

※

Ｃ＝ｍ$_0$ｃ$_0$＋ｍ$_1$ｃ$_1$＋・・・＋ｍ$_{K-1}$ｃ$_{K-1}$　…（ｈ）

素数Ｐ，Ｑを設定するステップと、

基数ベクトルＤ$_{Pi}$（０≦ｉ≦Ｋ－１）を整数ｄ$_{Pi}$を用いてＤ$_{Pi}$＝ｄ$_P$／ｄ$_{Pi}$（但し、ｄ$_P$＝ｄ$_{P0}$ｄ$_{P1}$…ｄ$_{PK-1}$（任意の２つの数ｄ$_{Pi}$，ｄ$_{Pj}$は互いに素））に設定するステップと、

基数ベクトルＤ$_{Qi}$（０≦ｉ≦Ｋ－１）を整数ｄ$_{Qi}$を用いてＤ$_{Qi}$＝ｄ$_Q$／ｄ$_{Qi}$（但し、ｄ$_Q$＝ｄ$_{Q0}$ｄ$_{Q1}$…ｄ$_{QK-1}$（任意の２つの数ｄ$_{Qi}$，ｄ$_{Qj}$は互いに素））に設定するステップと、

中国人の剰余定理を用いて、Ｐ，Ｑによる余りがそれぞれＤ$_{Pi}$，Ｄ$_{Qi}$となるような最小の整数Ｄ$_i$を導くステップと、

ｗ＜Ｎ（Ｎ＝ＰＱ）を満たすｗを選択し、式（ｋ）によ

り公開鍵ベクトルｃ＝（c_0，c_1，…，c_{K-1}）を求めるステップと、

$c_i \equiv wD_i \pmod N$　…（k）

＊

$C = m_0 c_0 + m_1 c_1 + \cdots + m_{K-1} c_{K-1}$　…（l）

暗号文Ｃに対して、法Ｐ，法Ｑにおいて、それぞれ中間復号文M_P，M_Qを式（ｍ），式（ｎ）のようにして求めるステップと、

$M_P \equiv w^{-1}C \pmod P$　…（m）

$M_Q \equiv w^{-1}C \pmod Q$　…（n）

この中間復号文M_P，M_Qを以下の式（ｏ），式（ｐ）により復号して余りのペア（$m_i^{(P)}$，$m_i^{(Q)}$）を求めるステップと、

$m_i^{(P)} \equiv M_P D_{Pi}^{-1} \pmod{d_{Pi}}$　…（o）

$m_i^{(Q)} \equiv M_Q D_{Qi}^{-1} \pmod{d_{Qi}}$　…（p）

求めた$m_i^{(P)}$，$m_i^{(Q)}$に中国人の剰余定理を適用して、平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）を求めるステップとを有することを特徴とする暗号化・復号方法。

【請求項９】　前記Ｎを法として前記暗号文Ｃを送るようにした請求項８記載の暗号化・復号方法。

【請求項１０】　複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１，２，３または５の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文を元の平文に復号する復号器とを備えることを特徴とする暗号通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、平文を暗号文に変換するための暗号化方法、及び、暗号文を元の平文に変換するための復号方法に関し、特に、積和型暗号に関する。

【０００２】

【従来の技術】高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

＊平文ベクトルｍと公開鍵ベクトルｃとの内積により、式（ｌ）に示す暗号文Ｃを作成するステップと、

【０００４】暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

【０００５】これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

【０００６】

【発明が解決しようとする課題】公開鍵暗号系の１つである積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。

【０００７】本発明は斯かる事情に鑑みてなされたものであり、高速な復号処理が可能である、積和型暗号に関する新規の暗号化方法及び復号方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】請求項１に係る暗号化方法は、平文をＫ分割した平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）と基数ベクトルＤ＝（D_0，D_1，…，D_{K-1}）とを用いて暗号文$C = m_0 D_0 + m_1 D_1 + \cdots + m_{K-1} D_{K-1}$を得る暗号化方法において、前記$D_i$（$0 \leq i \leq K-1$）を$D_i = d / d_i$（但し、$d = d_0 d_1 \cdots d_{K-1}$（任意の２つの数$d_i$，$d_j$は互いに素））に設定することを特徴とする。

【０００９】請求項２に係る暗号化方法は、平文をＫ分割した平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）と基数ベクトルＤ＝（D_0，D_1，…，D_{K-1}）とを用い

て暗号文$C=m_0 D_0+m_1 D_1+\cdots+m_{K-1} D_{K-1}$を得る暗号化方法において、前記$D_i$（$0\leqq i\leqq K-1$）を$D_i=(d/d_i)\cdot v_i$（但し、$d=d_0 d_1\cdots d_{K-1}$（任意の２つの数$d_i$，$d_j$は互いに素），$v_i$：乱数）に設定することを特徴とする。

【００１０】請求項３に係る暗号化方法は、請求項１において、乱数ベクトル$v=(v_0, v_1, \cdots, v_{K-1})$を用いて暗号文$C=m_0 v_0 D_0+m_1 v_1 D_1+\cdots+m_{K-1} v_{K-1} D_{K-1}$を得ることを特徴とする。

【００１１】請求項４に係る復号方法は、請求項１，２または３の何れかによって暗号化された暗号文Ｃを復号する復号方法であって、以下の式（ａ）により平文ベクトル$m=(m_0, m_1, \cdots, m_{K-1})$を求めることを特徴とする。

$$m_i \equiv C D_i^{-1} \pmod{d_i} \quad \cdots(a)$$

【００１２】請求項５に係る暗号化方法は、請求項１または２において、前記Ｋ個のd_iの集合を複数組準備

$$C=m_0 c_0+m_1 c_1+\cdots+m_{K-1} c_{K-1} \quad \cdots(c)$$

暗号文Ｃに対して、中間復号文Ｍを式（ｄ）のようにして求めるステップと、

$$M\equiv w^{-1}C \pmod{P} \quad \cdots(d)$$

この中間復号文Ｍを以下の式（ｅ）により復号して平文ベクトル$m=(m_0, m_1, \cdots, m_{K-1})$を求めるステップと

$$m_i \equiv M D_i^{-1} \pmod{d_i} \quad \cdots(e)$$

を有することを特徴とする。

【００１４】請求項７に係る暗号化・復号方法は、平文をＫ分割した平文ベクトル$m=(m_0, m_1, \cdots, m_{K-1})$と基数ベクトル$D=(D_0, D_1, \cdots, D_{K-1})$とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、

$$C=m_0 c_0+m_1 c_1+\cdots+m_{K-1} c_{K-1} \quad \cdots(h)$$

暗号文Ｃに対して、中間復号文Ｍを式（ｉ）のようにして求めるステップと、

$$M\equiv w^{-1}C \pmod{P} \quad \cdots(i)$$

この中間復号文Ｍを以下の式（ｊ）により復号して平文ベクトル$m=(m_0, m_1, \cdots, m_{K-1})$を求めるステップと

$$m_i \equiv M D_i^{-1} \pmod{d_i} \quad \cdots(j)$$

を有することを特徴とする。

【００１５】請求項８に係る暗号化・復号方法は、平文をＫ分割した平文ベクトル$m=(m_0, m_1, \cdots, m_{K-1})$と基数ベクトル$D=(D_0, D_1, \cdots, D_{K-1})$とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、素数Ｐ，Ｑを設定するステップと、基数ベクトルD_{Pi}（$0\leqq i\leqq$

＊し、それぞれの集合毎に暗号文を得るようにしたことを特徴とする。

【００１３】請求項６に係る暗号化・復号方法は、平文をＫ分割した平文ベクトル$m=(m_0, m_1, \cdots, m_{K-1})$と基数ベクトル$D=(D_0, D_1, \cdots, D_{K-1})$とを用いて前記平文を暗号文に変換し、その暗号文を元の平文に変換する暗号化・復号方法において、前記D_i（$0\leqq i\leqq K-1$）を整数d_iを用いてd/d_i（但し、$d=d_0 d_1\cdots d_{K-1}$（任意の２つの数d_i，d_jは互いに素））に設定するステップと、$w<P$（Ｐ：素数）を満たすｗを選択し、式（ｂ）により公開鍵ベクトル$c=(c_0, c_1, \cdots, c_{K-1})$を求めるステップと、

$$c_i \equiv w D_i \pmod{P} \quad \cdots(b)$$

平文ベクトルｍと公開鍵ベクトルｃとの内積により、式（ｃ）に示す暗号文Ｃを作成するステップと、

※前記D_i（$0\leqq i\leqq K-1$）を式（ｆ）にて設定するステップと、

$$D_i=(d/d_i)\cdot v_i \quad \cdots(f)$$

但し、v_i：乱数

d_i：整数

$d=d_0 d_1\cdots d_{K-1}$

（任意の２つの整数d_i，d_jは互いに素）

$w<P$（Ｐ：素数）を満たすｗを選択し、式（ｇ）により公開鍵ベクトル$c=(c_0, c_1, \cdots, c_{K-1})$を求めるステップと、

$$c_i \equiv w D_i \pmod{P} \quad \cdots(g)$$

平文ベクトルｍと公開鍵ベクトルｃとの内積により、式（ｈ）に示す暗号文Ｃを作成するステップと、

★Ｋ－１）を整数d_{Pi}を用いて$D_{Pi}=d_P/d_{Pi}$（但し、$d_P=d_{P0}d_{P1}\cdots d_{PK-1}$（任意の２つの数$d_{Pi}$，$d_{Pj}$は互いに素））に設定するステップと、基数ベクトル$D_{Qi}$（$0\leqq i\leqq K-1$）を整数$d_{Qi}$を用いて$D_{Qi}=d_Q/d_{Qi}$（但し、$d_Q=d_{Q0}d_{Q1}\cdots d_{QK-1}$（任意の２つの数$d_{Qi}$，$d_{Qj}$は互いに素））に設定するステップと、中国人の剰余定理を用いて、Ｐ，Ｑによる余りがそれぞれD_{Pi}，D_{Qi}となるような最小の整数D_iを導くステップと、$w<N$（$N=PQ$）を満たすｗを選択し、式（ｋ）により公開鍵ベクトル$c=(c_0, c_1, \cdots, c_{K-1})$を求めるステップと、

$$c_i \equiv w D_i \pmod{N} \quad \cdots(k)$$

平文ベクトルｍと公開鍵ベクトルｃとの内積により、式（ｌ）に示す暗号文Ｃを作成するステップと、

$$C=m_0 c_0+m_1 c_1+\cdots+m_{K-1} c_{K-1} \quad \cdots(l)$$

暗号文Ｃに対して、法Ｐ，法Ｑにおいて、それぞれ中間復号文M_P，M_Qを式（ｍ），式（ｎ）のようにして求めるステップと、

$$M_P \equiv w^{-1}C \pmod{P} \quad \cdots(m)$$

$$M_Q \equiv w^{-1}C \pmod{Q} \quad \cdots(n)$$

この中間復号文M_P，M_Qを以下の式（ｏ），式（ｐ）

により復号して余りのペア（$m_i^{(P)}$，$m_i^{(Q)}$）を求めるステップと、

$m_i^{(P)} \equiv M_P D_{Pi}^{-1} \pmod{d_{Pi}}$　…（o）

$m_i^{(Q)} \equiv M_Q D_{Qi}^{-1} \pmod{d_{Qi}}$　…（p）

求めた$m_i^{(P)}$，$m_i^{(Q)}$に中国人の剰余定理を適用して、平文ベクトルm＝（m_0，m_1，…，m_{K-1}）を求めるステップとを有することを特徴とする。

【００１６】請求項９に係る暗号化・復号方法は、請求項８において、前記Ｎを法として前記暗号文Ｃを送るようにしたことを特徴とする。

【００１７】請求項10に係る暗号通信システムは、複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１，２，３または５の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから＊

$$M = m_0 D_0 + m_1 D_1 + \cdots + m_{K-1} D_{K-1} \quad \cdots (3)$$

但し、メッセージベクトルmの各要素m_iは$m_i < d_i$を満たすように設定する。

【００２０】本発明では、このようにして、つまり、式（１）～式（３）を利用して、暗号文を作成する。

【００２１】基数を式（２）で与えた場合には、以下に示すアルゴリズムにより、整数Mからメッセージm＝（m_0，m_1，…，m_{K-1}）を復号することができる。この復号アルゴリズムを並列復号アルゴリズムという。

【００２２】〔並列復号アルゴリズム〕

unit　i（m_iの復号）

$m_i \equiv MD_i^{-1} \pmod{d_i}$

【００２３】このような概念に基づく暗号化手法とそれに対する復号方法とを、本発明の特徴とする。なお、具体的な手法については後述する。

【００２４】

【発明の実施の形態】以下、本発明の実施の形態について具体的に説明する。図１は、本発明による暗号化方法・復号方法をエンティティａ，ｂ間の情報通信に利用した状態を示す模式図である。図１の例では、一方のエンティティａが、暗号化器１にて平文ｘを暗号文Ｃに暗号化し、通信路３を介してその暗号文Ｃを他方のエンティティｂへ送信し、エンティティｂが、復号器２にてその暗号文Ｃを元の平文ｘに復号する場合を示している。　※

$$C = m_0 c_0 + m_1 c_1 + \cdots + m_{K-1} c_{K-1} \quad \cdots (6)$$

【００２７】エンティティｂ側では、以下のようにして復号処理が行われる。最初に、暗号文Ｃに対して、中間復号文Ｍを式（７）のようにして導く。

$M \equiv w^{-1}C \pmod{P}$　…（7）

【００２８】この中間復号文Ｍは、具体的には前記式（３）として与えられるので、前述の並列復号アルゴリズムによって復号できる。Ｋ重の並列処理が可能である場合には、２回の乗除算処理を実行するのに必要な時間で暗号文Ｃを高速に復号できる。また、本発明では、最上位の桁から順に（または最下位の桁から順に）メッセ

＊ら他方のエンティティへ送信する通信路と、送信された暗号文を元の平文に復号する復号器とを備えることを特徴とする。

【００１８】本発明の暗号化方法・復号方法の概念について、以下に説明する。Ｋ個の整数を要素とする集合｛d_i｝を考える。なお、この集合の任意の２つの要素は互いに素である。そして、式（１）に示すように、これらのＫ個の要素の積をｄとし、基数D_iを式（２）のように定義する。

$d = d_0 d_1 \cdots d_{K-1}$　…（1）

$D_i = d / d_i$　…（2）

【００１９】そして、メッセージm＝（m_0，m_1，…，m_{K-1}）を、基数D＝（D_0，D_1，…，D_{K-1}）を用いて、下記式（３）に示すように表記する。

※【００２５】（第１実施の形態）秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：｛d_i｝，Ｐ，ｗ

・公開鍵：｛c_i｝

前記式（２）のように基数を与える。この場合、基数ベクトル｛D_i｝は超増加数列ではなく、ＬＬＬ（Lenatra-Lenatra-Lovasz）法攻撃に強い。また、ｗ＜Ｐ（Ｐは大きな素数）を満たす整数ｗをランダムに選ぶ。また、メッセージベクトルmの各要素m_iは$m_i < d_i$を満たすように設定する。整数ｗを用いてＤの成分より、公開鍵ベクトルｃを式（４），（５）のように導く。

$c_i \equiv wD_i \pmod{P}$　…（4）

c＝（c_0，c_1，…，c_{K-1}）　…（5）

【００２６】また、$\mu < min(d_0, d_1, \cdots, d_{K-1})$なるμが各エンティティに公開される。エンティティａ側で、この公開されたμに基づいて、Ｋ次元のμ以下の大きさのメッセージベクトルに平文ｘを分割する。エンティティａ側で、メッセージベクトルmと公開鍵ベクトルｃとの内積を式（６）のように求めて、平文ｘを暗号化して暗号文Ｃを得る。作成された暗号文Ｃは通信路３を介してエンティティａからエンティティｂへ送信される。

ージベクトルの各要素を復号する必要はなく、任意の桁のメッセージ要素を自由に並列的に復号できるので、並列通信が可能となる。

【００２９】ところで、２つのd_i，d_jの組（d_i，d_j）を総当たり的に仮定すると、Ｐが露呈することになる。よって、実用上d_iは2^{32}程度に選ぶ必要がある。

【００３０】ここで、第１実施の形態における具体例を示す。

・秘密鍵

d＝（11，17，29）

D＝（17・29，29・11，11・17）

＝（493，319，187）

P＝59659

w＝25252

w^{-1}≡48633　（mod P）

（D_1，D_2，D_3は超増加数列でない）

・公開鍵

c≡wD≡（40164，1423，9063）　（mod P）

・暗号化

メッセージをm＝（４，６，８）とする。

C＝c・m＝241698

・復号

中間復号文Mを求め、並列復号アルゴリズムを用いて復号する。

M≡w^{-1}C≡5382　（mod 59659）

m_0≡5382・493 $^{-1}$≡４　（mod 11）

m_1＝5382・319 $^{-1}$≡６　（mod 17）

m_2＝5382・187 $^{-1}$≡８　（mod 29）

以上のようにして、メッセージm＝（４，６，８）を得る。

【００３１】（第２実施の形態）第１実施の形態に乱数を付加した第２実施の形態について説明する。第１実施の形態において、wとD_iとの積の総乗積を求めると、下記式（８）のようになってwとdとの多重積となるので、w，dが求まる可能性が皆無とは言えない。よって、第２実施の形態では、第１実施の形態での基数ベクトルに乱数を掛け合わせたものを基数ベクトルとして使用することにより安全性を強化する。

【００３２】

【数１】

$$\prod_{i=0}^{\kappa-1} wD_i = w^{\kappa} \cdot \frac{d^{\kappa}}{d}$$

$$= w^{\kappa} d^{\kappa-1} \qquad \cdots (8)$$

【００３３】秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：$\{d_i\}$，$\{v_i\}$，P，w

・公開鍵：$\{c_i\}$

同程度の大きさの乱数v_0，v_1，…，v_{K-1}を用いて、基数D_iを式（９）のように与える。但し、d_iとv_iとは互いに素であるとする。

D_i＝（d／d_i）・v_i　　…（９）

【００３４】整数wを用いて、第１実施の形態と同様に、公開鍵ベクトルcを以下の式（10），式（11）のように求める。

c_i≡wD_i　（mod P）　　…（10）

c＝（c_0，c_1，…，c_{K-1}）　　…（11）

【００３５】メッセージベクトルmと公開鍵ベクトルcとの内積により、第１実施の形態と同様に（前記式

（６），、暗号文Cを得る。

【００３６】復号処理は、以下のようにして行われる。暗号文Cに対して、中間復号文Mを式（12）のようにして求める。

M≡w^{-1}C　（mod P）　　…（12）

この中間復号文Mは、具体的には前記式（３）として与えられるので、第１実施の形態と同様に、並列復号アルゴリズムによって復号される。

【００３７】ここで、第２実施の形態における具体例を示す。

・秘密鍵

d＝（11，17，29）

v＝（８，７，５）

D＝（2465，2233，1496）

P＝59659

w＝25252

w^{-1}≡48633　（mod P）

・公開鍵

c≡wD

≡（21843，9961，12845）　（mod P）

・暗号化

メッセージをm＝（７，８，９）とする。

C＝c・m

＝348194

・復号

中間復号文Mを求め、並列復号アルゴリズムを用いて復号する。

M≡w^{-1}C≡48583　（mod 59659）

m_0≡48583・2465^{-1}≡７　（mod 11）

m_1＝48583・2233^{-1}≡８　（mod 17）

m_2＝48583・1496^{-1}≡９　（mod 29）

以上のようにして、メッセージm＝（７，８，９）を得る。

【００３８】（第３実施の形態）第２実施の形態では、基数ベクトル自体に乱数を組み込むようにしたが、第１実施の形態と同じ基数ベクトルを使用し、暗号文Cを作成する段階で乱数v_0，v_1，…，v_{K-1}を付加するようにすることもできる。この場合の暗号文Cは、第２実施の形態と同じ形となる。

【００３９】（第４実施の形態）第１実施の形態で基数ベクトルを多重化した第４実施の形態について説明する。第４実施の形態は、第１実施の形態による基数ベクトル$\{D_i\}$を２つの法それぞれにおいて設定し、中国人の剰余定理を利用した暗号化・復号方法である。

【００４０】秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：$\{d_{Pi}\}$，$\{d_{Qi}\}$，P，Q，N，w

・公開鍵：$\{c_i\}$

２つの大きな素数P，Qを選択し、それらの積をNとする。第１実施の形態におけるK個の要素からなる集合

$\{d_i\}$ を２通り準備し、$\{d_{Pi}\}$，$\{d_{Qi}\}$ とする。また、それらより生成した基数を $\{D_{Pi}\}$，$\{D_{Qi}\}$ とする。中国人の剰余定理を用いて、Ｐ，Ｑによる余りがそれぞれD_{Pi}，D_{Qi}となるような最小の整数D_i を導き、それを基数とする。

【００４１】Ｎを法として、秘密の乱数ｗを用いて、第１実施の形態と同様に、公開鍵ベクトルｃを以下の式（13），式（14）のように求める。

$$c_i \equiv wD_i \pmod N \quad \cdots (13)$$

$$c = (c_0, c_1, \cdots, c_{K-1}) \quad \cdots (14)$$

【００４２】メッセージベクトルｍと公開鍵ベクトルｃ＊との内積により、第１実施の形態と同様に（前記式（６））、暗号文Ｃを得る。

$$M_P = m_0^{(P)} D_{P0} + m_1^{(P)} D_{P1} + \cdots + m_{K-1}^{(P)} D_{PK-1} \quad \cdots (17)$$

$$M_Q = m_0^{(Q)} D_{Q0} + m_1^{(Q)} D_{Q1} + \cdots + m_{K-1}^{(Q)} D_{QK-1} \quad \cdots (18)$$

$$m_i \equiv m_i^{(P)} \pmod{d_{Pi}} \quad \cdots (19)$$

$$m_i \equiv m_i^{(Q)} \pmod{d_{Qi}} \quad \cdots (20)$$

【００４３】復号処理は、以下のようにして行われる。暗号文Ｃに対して、法Ｐ，法Ｑにおいて、それぞれ中間復号文M_P，M_Q を式（15），式（16）のようにして導く。

$$M_P \equiv w^{-1}C \pmod P \quad \cdots (15)$$

$$M_Q \equiv w^{-1}C \pmod Q \quad \cdots (16)$$

【００４４】各中間復号文M_P，M_Q に関して、式（17），式（18）が成立する。但し、m_i は、式（19），式（20）の何れかであるとする。

【００４５】M_P，M_Q に対して、並列復号アルゴリズムを適用することによって、余りのペア（$m_i^{(P)}$，$m_i^{(Q)}$）を導くことができる。これらに対して中国人の剰余定理を適用すると、メッセージ$m_i < lcm(d_{Pi}, d_{Qi})$ を復号することができる。

【００４６】ここで、第４実施の形態における具体例を示す。

・秘密鍵

$d_P = (11, 17, 29)$

$d_Q = (13, 19, 23)$

$D_P = (493, 319, 187)$

$D_Q = (437, 299, 247)$

$D = (946872238594, 409641492482, 772314923252)$

$P = 1042183$

$Q = 960119$

$N = 1000619699777$

$w = 947284758293$

$w^{-1} \equiv 337608855274 \pmod N$

・公開鍵

$c \equiv wD \equiv (940952460514, 717925054865, 870712563437) \pmod N$

・暗号化

メッセージをｍ＝（45，67，89）とする。

$C = c \cdot m = 167937257544978$

・復号

中間復号文M_P，M_Q を求め、並列復号アルゴリズムを用いる。

$M_P \equiv w^{-1}C \equiv 60201 \pmod{1042183}$

$M_Q \equiv w^{-1}C \equiv 61681 \pmod{9600119}$

$m_0^{(P)} \equiv M_P \cdot 493^{-1} \equiv 1 \pmod{11}$

$m_1^{(P)} \equiv M_P \cdot 319^{-1} \equiv 16 \pmod{17}$

$m_2^{(P)} = M_P \cdot 187^{-1} \equiv 2 \pmod{29}$

※$m_0^{(Q)} \equiv M_Q \cdot 437^{-1} \equiv 6 \pmod{13}$

$m_1^{(Q)} \equiv M_Q \cdot 299^{-1} \equiv 10 \pmod{19}$

$m_2^{(Q)} = M_Q \cdot 247^{-1} \equiv 20 \pmod{23}$

（$m_0^{(P)}$，$m_0^{(Q)}$）から中国人の剰余定理により、$m_0 = 45$を求める。同様に、（$m_1^{(P)}$，$m_1^{(Q)}$），（$m_2^{(P)}$，$m_2^{(Q)}$），から$m_1 = 67$，$m_2 = 89$を求める。以下のようにして、メッセージｍ＝（45，67，89）を得る。

【００４７】なお、合成数Ｎを法とする第４実施の形態のような多重化方式では、Ｎの素因数分解が困難である場合、Ｎを公開しても安全と考えられる。よって、そのような場合には、Ｎを法として求めた暗号文Ｃを送付することにより、暗号化効率が向上する。

【００４８】（第５実施の形態）第５実施の形態は、第４実施の形態に乱数を付加した暗号方式、言い換えると、第２実施の形態で基数ベクトルを多重化した暗号方式である。なお、この第５実施の形態については、前述の第１～第４実施の形態を参照すれば容易にその内容が理解されるので、詳細な説明は省略する。

【００４９】（第６実施の形態）第４実施の形態では、２個の素数を用いた多重化方式について説明したが、３個以上の素数を用いて多重化するようにしても良い。第６実施の形態ではＬ個の素数P_0，P_1，…，P_{L-1} を用いる場合について説明する。なお、$P_0 = P$，$P_1 = Q$とすれば、第４実施の形態と一致する。

【００５０】秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：$\{P_j\}$，$\{r_{j,i}\}$，ｗ

・公開鍵：$\{c_i\}$

素数P_j（ｊ＝０，１，・・・，Ｌ－１）に対し、第４実施の形態におけるD_P，D_Q と同様なベクトルD_{Pj}を式（21）のように与える。

※ D_{Pj}

13

14

$$= (r_j / r_{j,0},\ r_j / r_{j,1},\ \cdots,\ r_j / r_{j,j},\ \cdots,\ r_j / r_{j,K-1}) \quad \cdots (21)$$

但し、$r_j = r_{j,0}\ r_{j,1} \cdots r_{j,K-1}$

【００５１】ここで、中国人の剰余定理を適用することにより、式（22）のようになる最小の整数をD_iとして、基数とする。

$$D_i \equiv D_{Pj,i} \pmod{P_j} \quad \cdots (22)$$

そして、$N = P_0\ P_1 \cdots P_{L-1}$を法として、第１実施の形態と同様に公開鍵ｃを準備する。

【００５２】第６実施の形態では、第１実施の形態と比べて、いわば２次元的な構造が組み込まれる。このことによって、次のような効果が期待される。

（１）Ｋ＝Ｌとした場合、K^2個のパラメータを用いてはじめてメッセージが復号される。次元数Ｋを同一にして比較した場合、より安全なシステムになっている。

（２）同様にＫ＝Ｌとした場合、式（23）に示すD_{P0}をｊ回巡回置換したベクトルをD_{Pj}として用いると、回路の単純化が可能となる。

$$D_{P0} = (r_0 / r_{0,0},\ r_0 / r_{0,1},\ \cdots,\ r_0 / r_{0,K-1}) \quad \cdots (23)$$

【００５３】なお、この第６実施の形態において、$r_{j,i}$を16ビット程度、Ｋ＝Ｌ＝８とした場合、公開鍵サイズは約8.2 キロビット、秘密パラメータ数は74となる。

【００５４】

【発明の効果】以上のように、本発明では、暗号化する際の基数D_iを$D_i = d / d_i$（但し、$d = d_0\ d_1 \cdots d_{K-1}$）に設定するようにしたので、平文ベクトルの各要素を並列的に復号でき、簡単な装置構成にて高速な復号を行うことができる。この結果、積和型暗号の実用化の道を開くことに、本発明は大いに寄与できる。

【図面の簡単な説明】

【図１】２人のエンティティ間における情報の通信状態を示す模式図である。

【符号の説明】

１　暗号化器

２　復号器

３　通信路

ａ，ｂ　エンティティ

【図１】